CAE Tech Talk

15 December 2022

The Rise of Side Channel Attacks: the case of wireless and mobile systems (1:00 – 1:50 pm EST)

Enhancing Finger Photo Presentation Attack Detection for Secure Smartphone Unlock (2:00 – 2:50 pm EST)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. Capitol Technology University (CTU) hosts the presentations using Zoom which employs slides, VOIP, and chat for live interaction. Just log in as "Guest" and enjoy the presentation(s).

Below is a description of the presentations and logistics of attendance:

PRESENTATION #1

Topic: The Rise of Side Channel Attacks: the case of wireless and mobile systems

Time: 1:00pm – 1:50 pm EST

Location: https://captechu.zoom.us/j/664120328

Just log in as "Guest" and enter your name. No password required.

Presenter(s): Guevara Noubir, Northeastern University

Description: Over the last decade, security and privacy has became a major concern for organizations, governments, and society. This resulted in extensive efforts to develop and deploy a wide variety of hardware and software defense mechanisms ranging from network security protocols, secure computing platforms, to usable security and policies. As the low-hanging vulnerabilities became harder to exploit, side-channel attacks started receiving more attention from the larger security community. The research community has been very prolific in discovering a wide variety of exploitable side-channel attacks. In this talk, we focus on side-channels in wireless and mobile systems. We discuss their unique features and root cause such

as resource constraints, inherent emissions, couplings and systems optimization. We review several recent attacks from our own work and others to illustrate the origins and risks. We also discuss defense approaches and their limitations in terms of effectiveness and realism.

PRESENTATION #2

Topic: Enhancing Finger Photo Presentation Attack Detection for Secure Smartphone Unlock

Time: 2:00pm – 2:50 pm EST

Location: https://captechu.zoom.us/j/664120328

Just log in as "Guest" and enter your name. No password required.

Presenter(s): Emanuela Marasco, George Mason University

Description: Finger photo recognition represents a promising touchless technology that offers portable and hygienic authentication solutions in smartphones, eliminating physical contact. Public spaces, such as banks and staff-less stores, benefit from contactless authentication considering the current public health sphere.

The user captures the image of his or her own finger by using the camera integrated in a mobile device. Although recent research has pushed boundaries of finger photo matching, the security of this biometric methodology still represents a concern.

Existing systems have been proven to be vulnerable to print attacks, realized by presenting in front of the camera a color paper-printout, and photo attacks, that consist in displaying the original image in front of the capturing device. These threats are referred to as presentation attacks (PAs).

The proposed research aims to improve the performance of finger photo presentation attack detection (PAD) algorithms by investigating deep fusion strategies to combine deep representations obtained from different color spaces. In this work, spoofness is described by combining different color models.

The proposed framework integrates multiple convolutional neural networks (CNNs), each trained using patches extracted from a specific color model and centered around minutiae points.

Experiments were carried out on a publicly available database of spoofed finger photos obtained from the IIITD Smartphone Finger photo Database with spoof data, including printouts and various display attacks.

The results show that deep fusion of the best color models improved the robustness of the PAD system and competes with the state-of-the-art.

CAE Tech Talks are recorded; view them here: https://www.caecommunity.org/resources/cae-tech-talk-resources

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov